Contents

Attacks

Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks ................................................. 3
  Amin Kharraz, William Robertson, Davide Balzarotti, Leyla Bilge, and Engin Kirda

“Nice Boots!” - A Large-Scale Analysis of Bootkits and New Ways to Stop Them ........................................ 25
  Bernhard Grill, Andrei Bacs, Christian Platzer, and Herbert Bos

C5: Cross-Cores Cache Covert Channel ................................................. 46
  Clémentine Maurice, Christoph Neumann, Olivier Heen, and Aurélien Francillon

Attack Detection

Intrusion Detection for Airborne Communication Using PHY-Layer Information ............................................. 67
  Martin Strohmeier, Vincent Lenders, and Ivan Martinovic

That Ain’t You: Blocking Spearphishing Through Behavioral Modelling ............................................. 78
  Gianluca Stringhini and Olivier Thonnard

Robust and Effective Malware Detection Through Quantitative Data Flow Graph Metrics ..................................... 98
  Tobias Wüchner, Martín Ochoa, and Alexander Pretschner

Binary Analysis and Mobile Malware Protection

Jackdaw: Towards Automatic Reverse Engineering of Large Datasets of Binaries ........................................... 121
  Mario Polino, Andrea Scorti, Federico Maggi, and Stefano Zanero

Fine-Grained Control-Flow Integrity Through Binary Hardening ............................................. 144
  Mathias Payer, Antonio Barresi, and Thomas R. Gross

Powerslave: Analyzing the Energy Consumption of Mobile Antivirus Software ........................................... 165
  Iasonas Polakis, Michalis Diamantaris, Thanasis Petsas, Federico Maggi, and Sotiris Ioannidis
Social Networks and Large-Scale Attacks

The Role of Cloud Services in Malicious Software: Trends and Insights  
Xiao Han, Nizar Kheir, and Davide Balzarotti

Capturing DDoS Attack Dynamics Behind the Scenes  
An Wang, Aziz Mohaisen, Wentao Chang, and Songqing Chen

Quit Playing Games with My Heart: Understanding Online Dating Scams  
JingMin Huang, Gianluca Stringhini, and Peng Yong

Web and Mobile Security

More Guidelines Than Rules: CSRF Vulnerabilities from Noncompliant OAuth 2.0 Implementations  
Ethan Shernan, Henry Carter, Dave Tian, Patrick Traynor, and Kevin Butler

May I? - Content Security Policy Endorsement for Browser Extensions  
Daniel Hausknecht, Jonas Magazinius, and Andrei Sabelfeld

On the Security and Engineering Implications of Finer-Grained Access Controls for Android Developers and Users  
Yanick Fratantonio, Antonio Bianchi, William Robertson, Manuel Egele, Christopher Kruegel, Engin Kirda, and Giovanni Vigna

Provenance and Data Sharing

Identifying Intrusion Infections via Probabilistic Inference on Bayesian Network  
Yuan Yang, Zhongmin Cai, Weixuan Mao, and Zhihai Yang

Controlled Data Sharing for Collaborative Predictive Blacklisting  
Julien Freudiger, Emiliano De Cristofaro, and Alejandro E. Brito

Author Index
Detection of Intrusions and Malware, and Vulnerability Assessment
12th International Conference, DIMVA 2015, Milan, Italy, July 9-10, 2015, Proceedings
Almgren, M.; Gulisano, V.; Maggi, F. (Eds.)
2015, XII, 351 p. 98 illus., Softcover
ISBN: 978-3-319-20549-6